PRELIMINARY AMENDMENT

AMENDMENTS TO THE SPECIFICATION

Amend the specification by adding before the first line the sentence:

This application is a National Stage application of PCT/US2003/026834 filed August 28, 2003.

Please amend paragraph [153] as follows:

[153] Each node *w* **902** of the tree, including the leaf nodes are assigned a secret key sk_w by the authorizer. To decrypt a message encrypted using PK during period *i*, only key $ski_{<i>}$ is needed. In addition, given key sk_w ~~sk_{ew} **903**~~, it is possible to efficiently derive descendant keys ~~se_{ow} **904**~~ sk_{w0} and sk_{w1} ~~**905**~~ for descendant nodes w_0 904 and w_1 905 and the descendants derived ~~from these keys~~of these nodes. However, given PK and i, and without ~~sk_{ew}~~ sk_w for all prefixes w of $< i >$, it is infeasible to derive $s_{ki<i>}$ or to decrypt messages encrypted during time-periods up to including *i*.

Please add the following Abstract of the Disclosure:

The present invention provides methods for sending a digital message from a sender to a recipient in a public-key based cryptosystem comprising an authorizer. The authorizer can be a single entity or comprise a hierarchical or distributed entity. The present invention allows communication of messages by an efficient protocol, not involving key status queries or key escrow, where a message recipient can decrypt a message from a message sender only if the recipient possesses up-to-date authority from the authorizer. The invention allows such communications in a system comprising a large number (e.g. millions) of users.